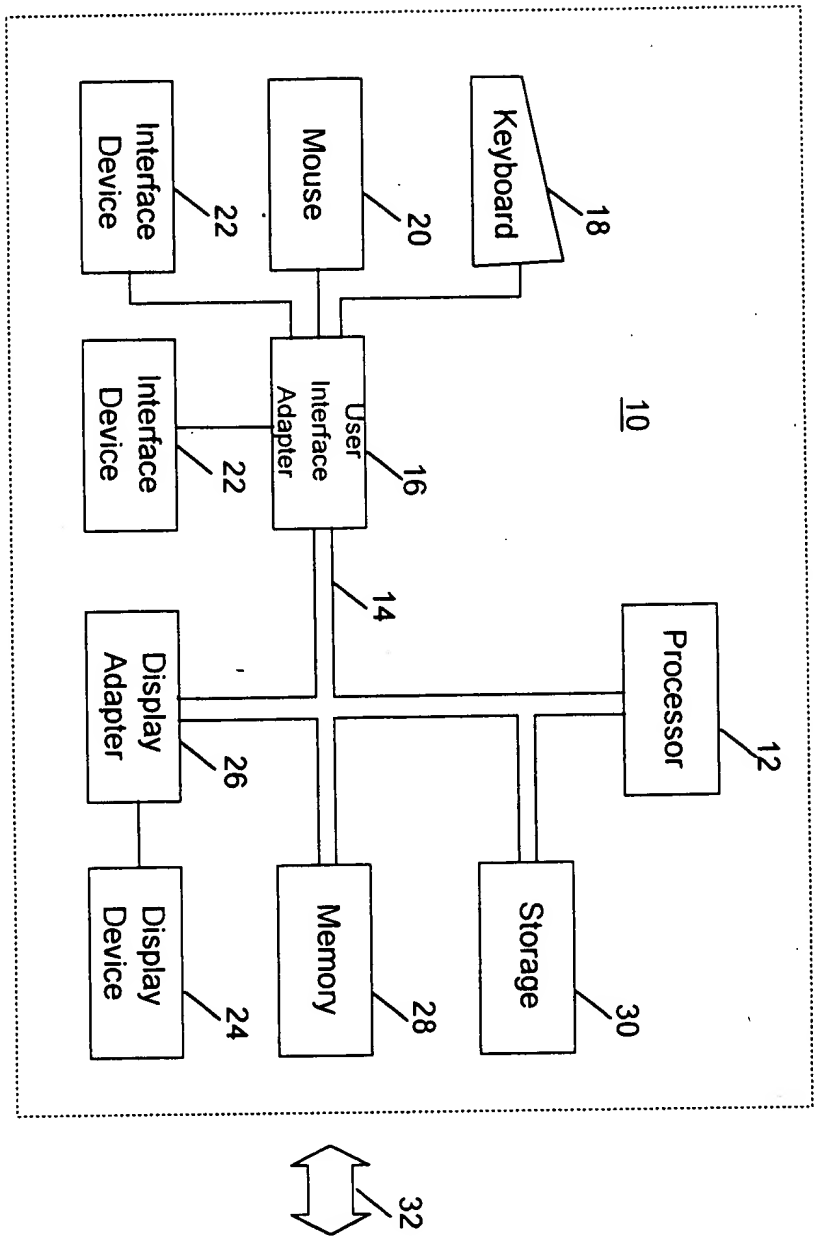


Fig. 1

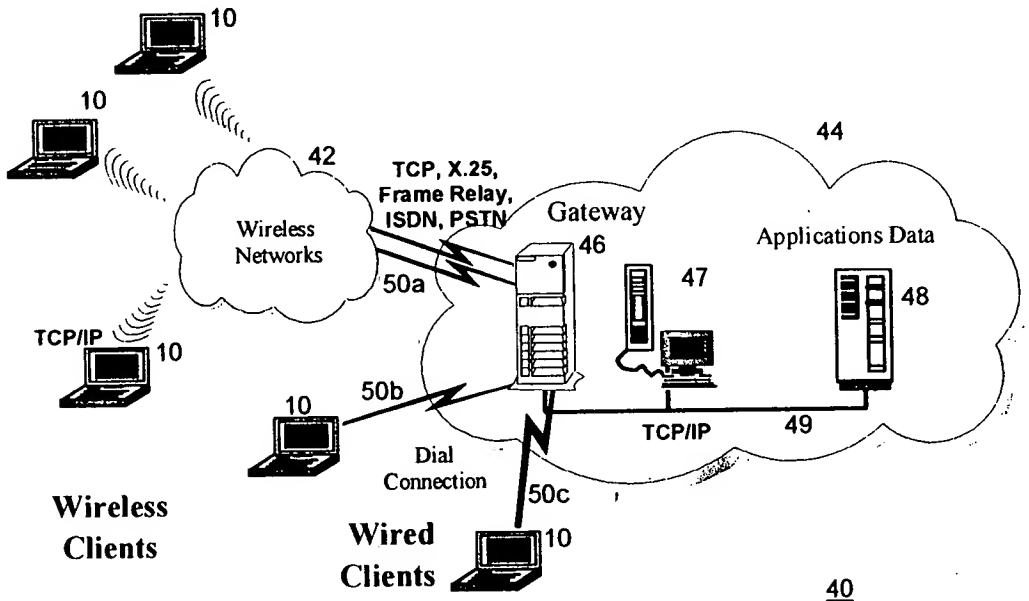


Fig. 2
(Prior Art)

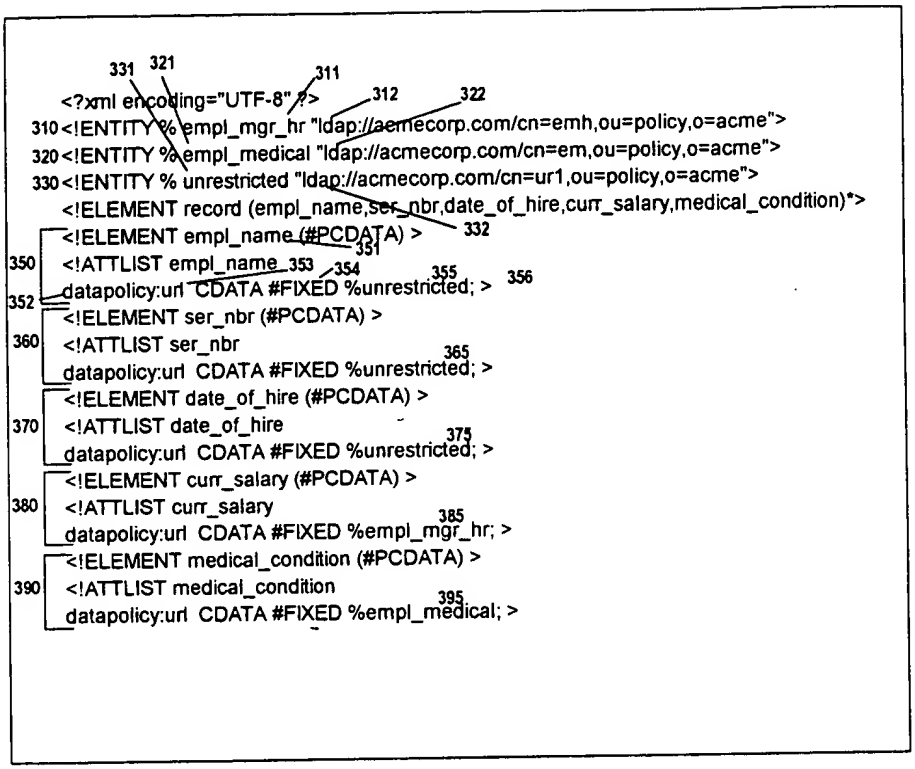


Fig. 3

400

```
<? xml version="1.0"  encoding ="UTF-8" ?>                                    405
<!DOCTYPE record SYSTEM  "ldap://acmecorp.com/cn=personnel,ou=dtd,o=acme?xmlProperty" >
<empl_name>
John Q. Smith                                                                 402
</empl_name>
<ser_nbr>
E135246                                                                       404
</ser_nbr>
<date_of_hire>
01/01/1980                                                                    406
</date_of_hire>
<curr_salary>
3395.00                                                                       408
</curr_salary>
<medical_condition>
diabetic                                                                      410
</medical_condition>
```

Fig. 4A

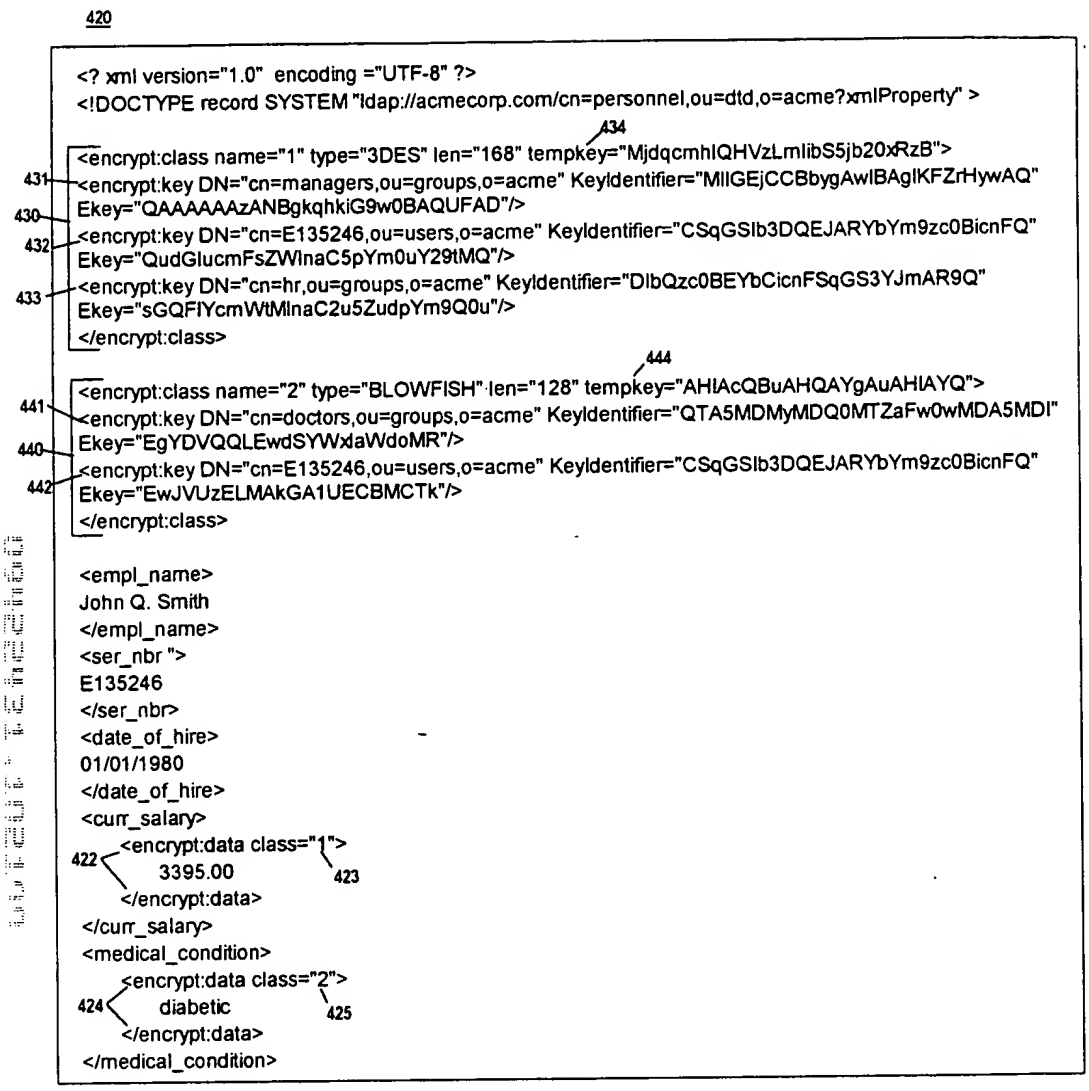


Fig. 4B

450

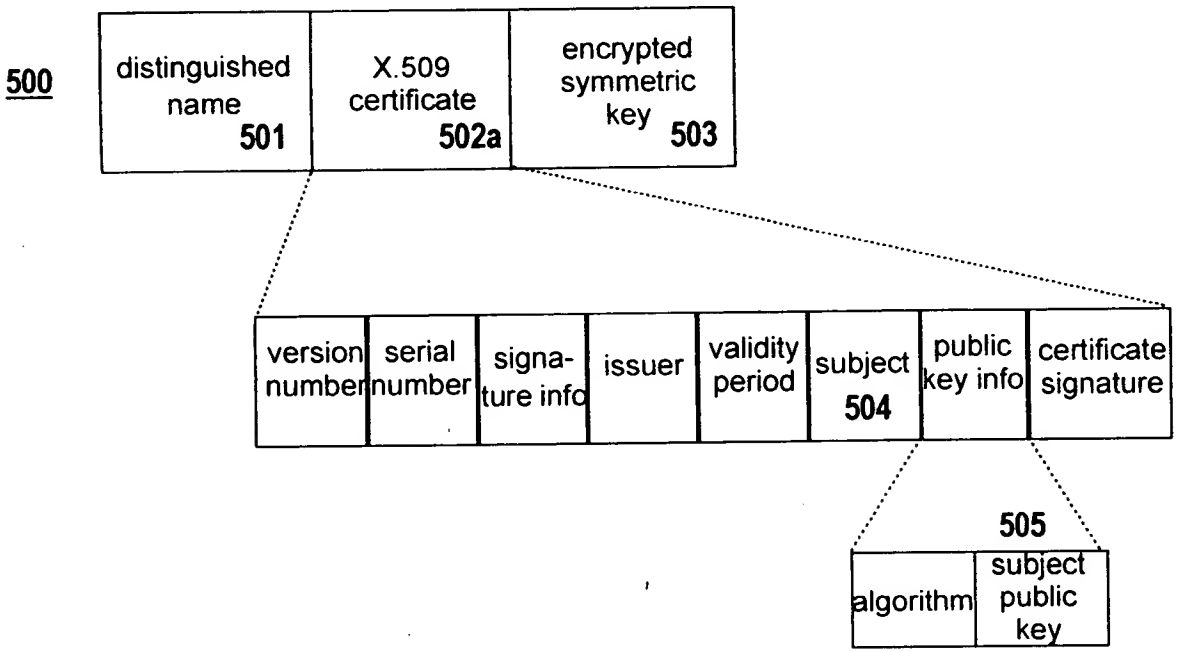
```
<? xml version="1.0"  encoding ="UTF-8" ?>
<!DOCTYPE record SYSTEM "ldap://acmecorp.com/cn=personnel,ou=dtd,o=acme?xmlProperty" >
<encrypt:class name="1" type="3DES" len="168">                                   (463, 470, 471)
<encrypt:key DN="cn=managers,ou=groups,o=acme" KeyIdentifier="MIIGEjCCBbygAwIBAgIKFZrHywAQ"   (464)
Ekey="QAAAAAAzANBgkqhkiG9w0BAQUFAD"/> 475
<encrypt:key DN="cn=E135246,ou=users,o=acme" KeyIdentifier="CSqGSIb3DQEJARYbYm9zc0BicnFQ"     (465)
Ekey="QudGlucmFsZWlnaC5pYm0uY29tMQ"/> 476                                        } 461
<encrypt:key DN="cn=hr,ou=groups,o=acme" KeyIdentifier="DIbQzc0BEYbCicnFSqGS3YJmAR9Q"
Ekey="dpYmGmFsZWaCc50u9ntMYlu2QuQ"/>                                             (460)
</encrypt:class>                                                                 (472, 473)

<encrypt:class name="2" type="BLOWFISH" len="128">
<encrypt:key DN="cn=doctors,ou=groups,o=acme" KeyIdentifier="QTA5MDMyMDQ0MTZaFw0wMDA5MDI"
Ekey="EgYDVQQLEwdSYWxlaWdoMR"/>                                                  } 462
<encrypt:key DN="cn=E135246,ou=users,o=acme" KeyIdentifier="CSqGSIb3DQEJARYbYm9zc0BicnFQ"
Ekey="EwJVUzELMAkGA1UECBMCTk"/>
</encrypt:class>

<empl_name>
John Q. Smith
</empl_name>
<ser_nbr ">
E135246
</ser_nbr>
<date_of_hire>
01/01/1980
</date_of_hire>
<curr_salary>
    <encrypt:data class="1">                                                     (456)
        Ym0uY29tMQ                                                               (453)
    </encrypt:data>                                                              } 452
</curr_salary>
<medical_condition>
    <encrypt:data class="2">
        MxDDAKBgNVB                                                              (455)
    </encrypt:data>                                                              } 454
</medical_condition>
```

Fig. 4C

Key Object - internal



Key Object - transmitted

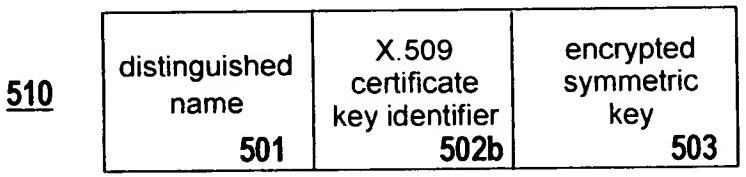


Fig. 5A

preprocessingKeyClass Object 520

encryption strength 521	key class object 522	plaintext symmetric key 523

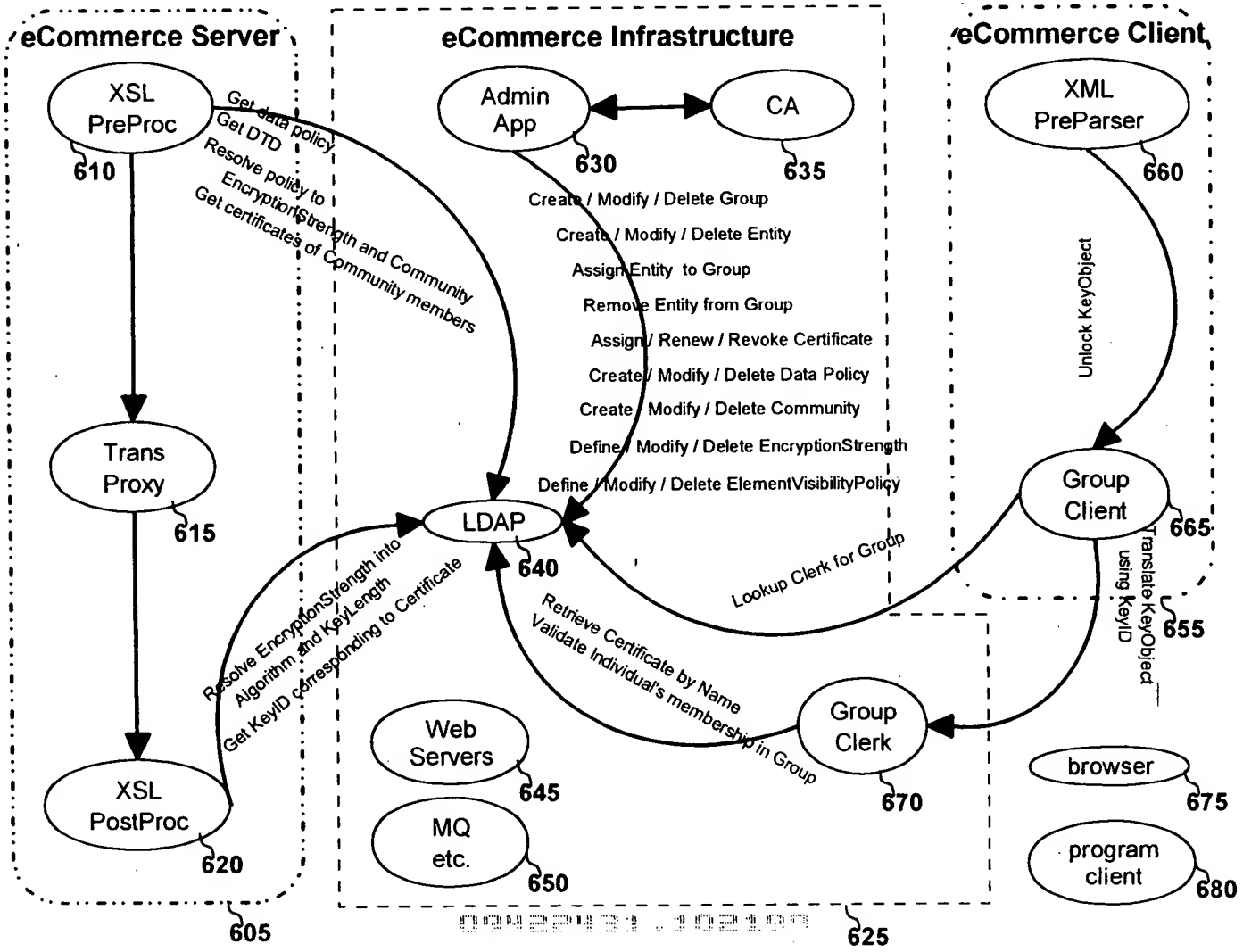
Fig. 5B

keyClass Object 530

class identifier 531	encryption algorithm identifier 532	key length 533	optional hints for algorithm 534	key object 1 535	key object 2 536	...	key object N 539

Fig. 5C

Fig. 6



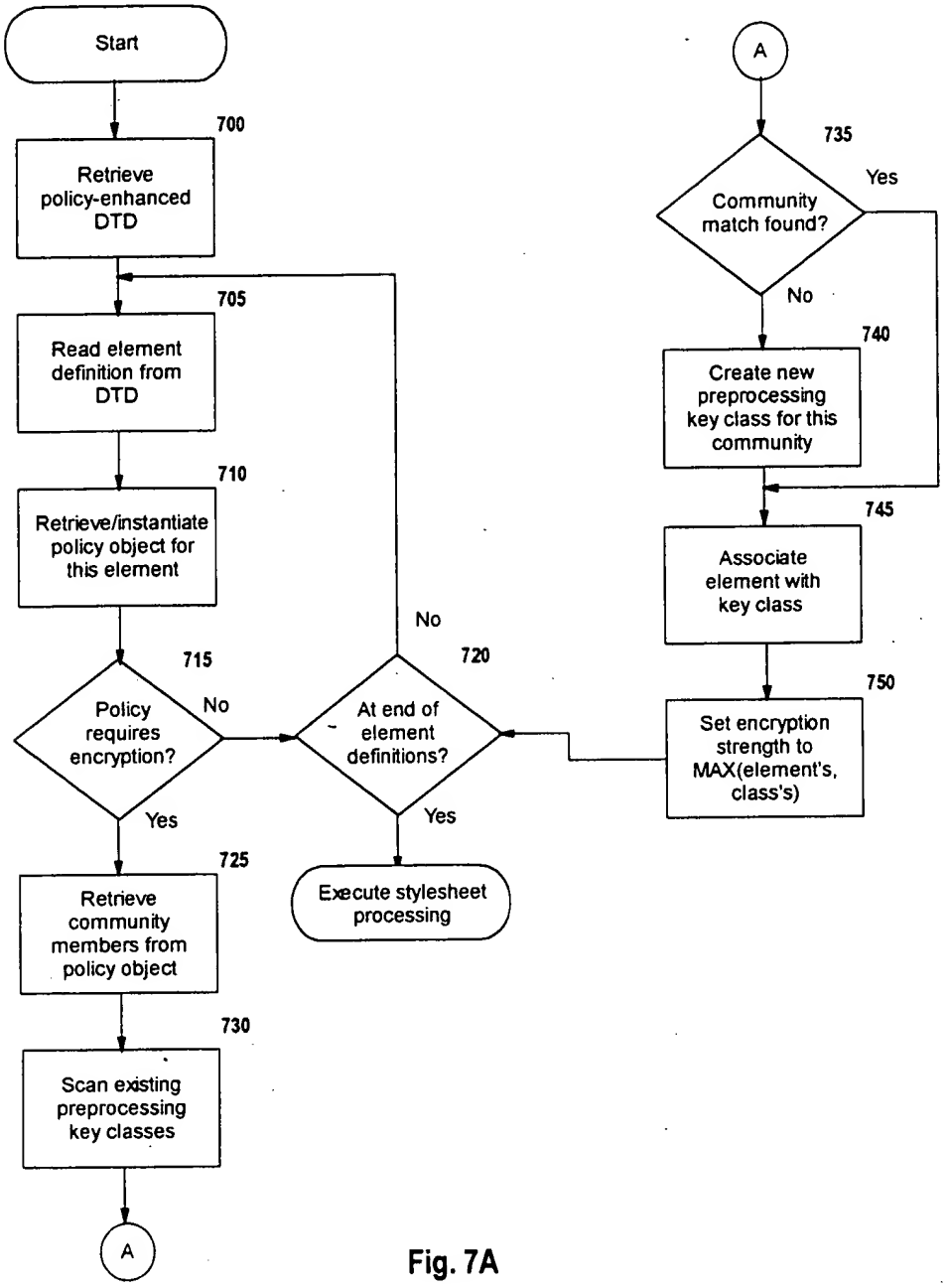


Fig. 7A

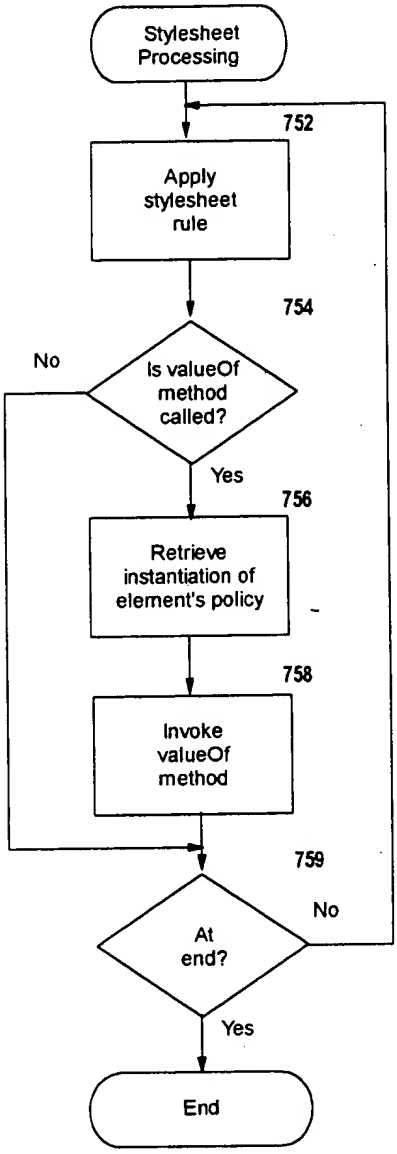

Stylesheet Processing
752
Apply stylesheet rule
754
No
Is valueOf method called?
Yes
756
Retrieve instantiation of element's policy
758
Invoke valueOf method
759
No
At end?
Yes
End

Fig. 7B

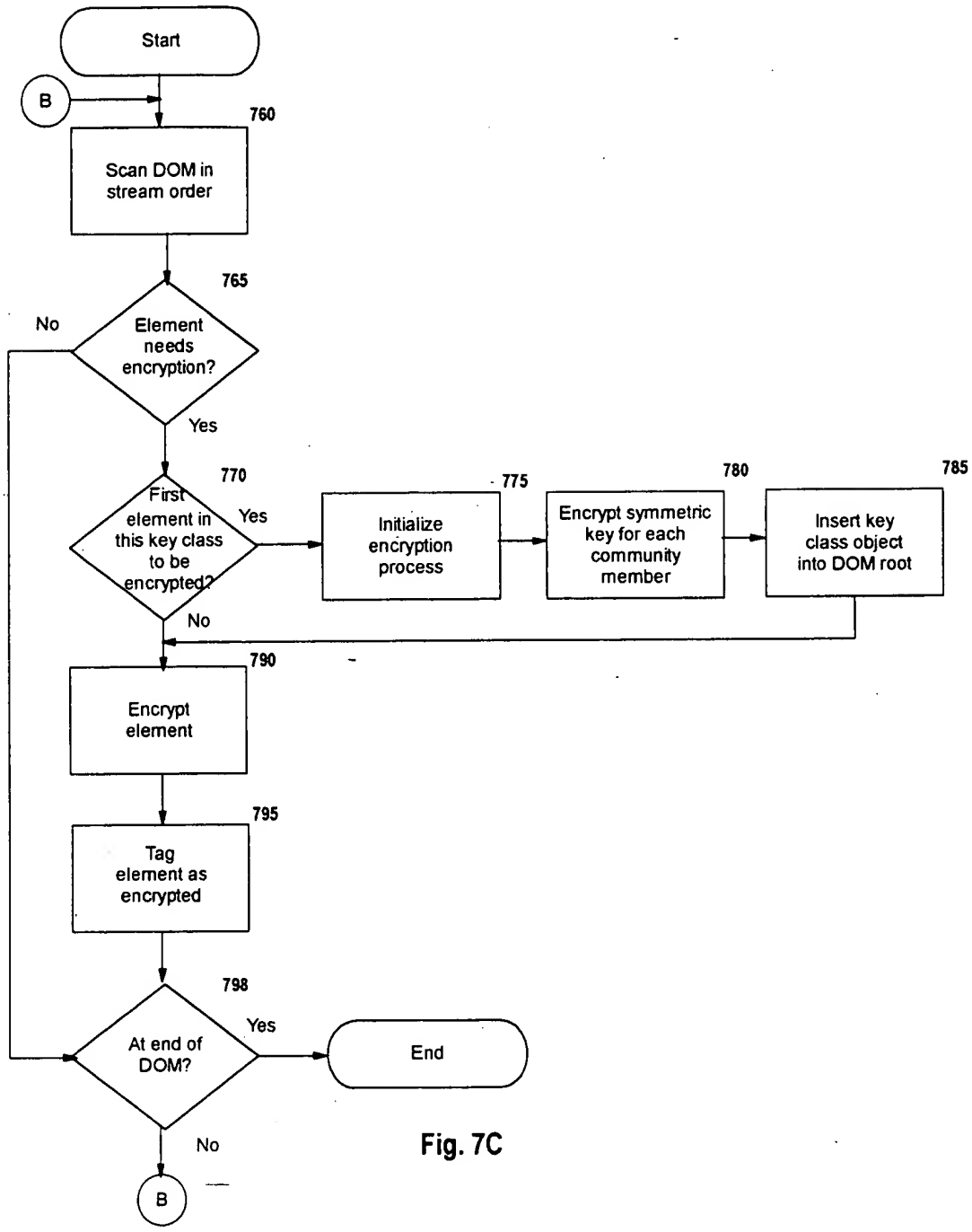

Start
B
760
Scan DOM in stream order
765
Element needs encryption?
No
Yes
770
First element in this key class to be encrypted?
Yes
775
Initialize encryption process
780
Encrypt symmetric key for each community member
785
Insert key class object into DOM root
No
790
Encrypt element
795
Tag element as encrypted
798
At end of DOM?
Yes
End
No
B

Fig. 7C

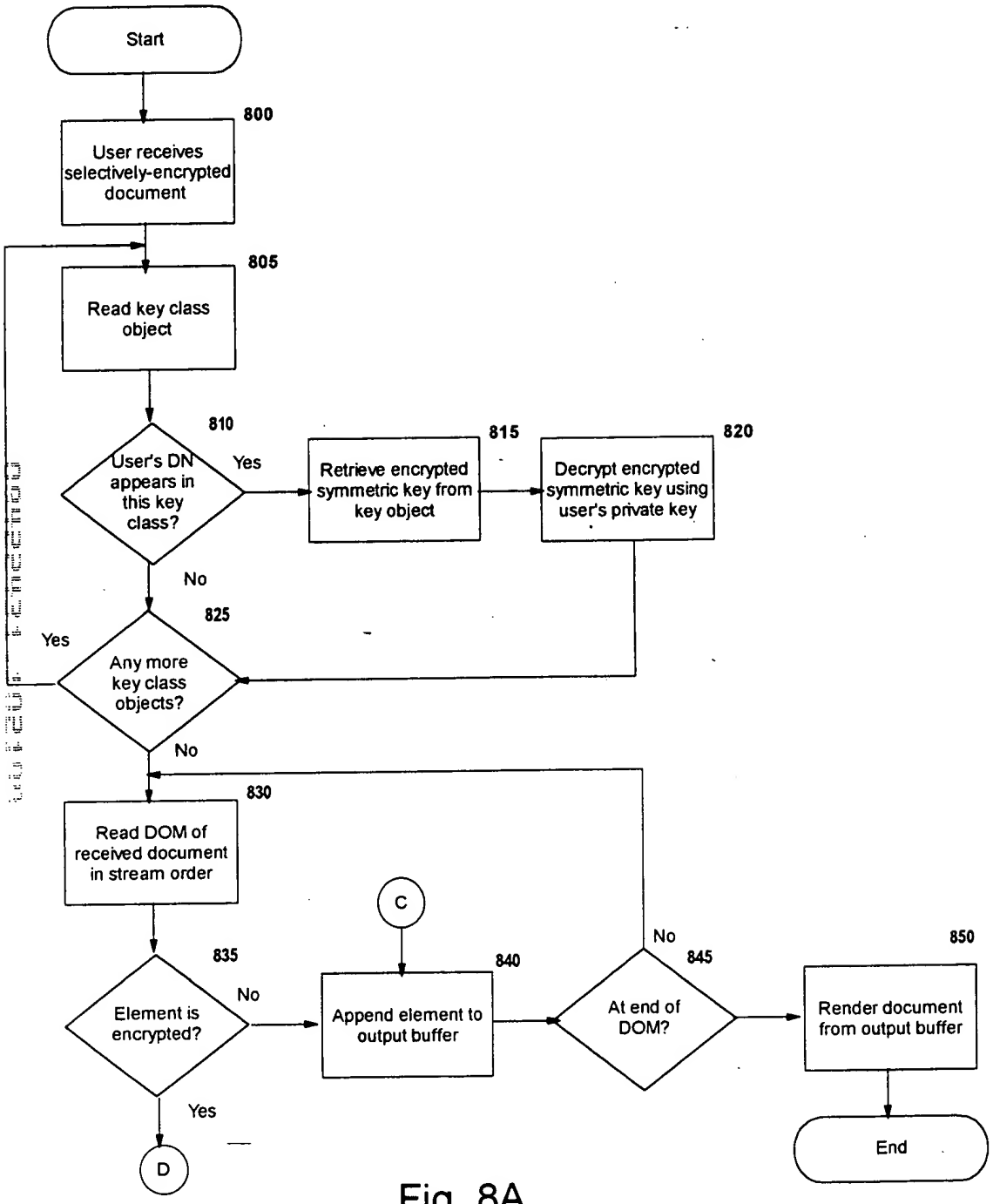

Start
800
User receives selectively-encrypted document
805
Read key class object
810
User's DN appears in this key class?
Yes
815
Retrieve encrypted symmetric key from key object
820
Decrypt encrypted symmetric key using user's private key
No
825
Any more key class objects?
Yes
No
830
Read DOM of received document in stream order
C
835
Element is encrypted?
No
840
Append element to output buffer
845
At end of DOM?
No
850
Render document from output buffer
Yes
D
End

Fig. 8A

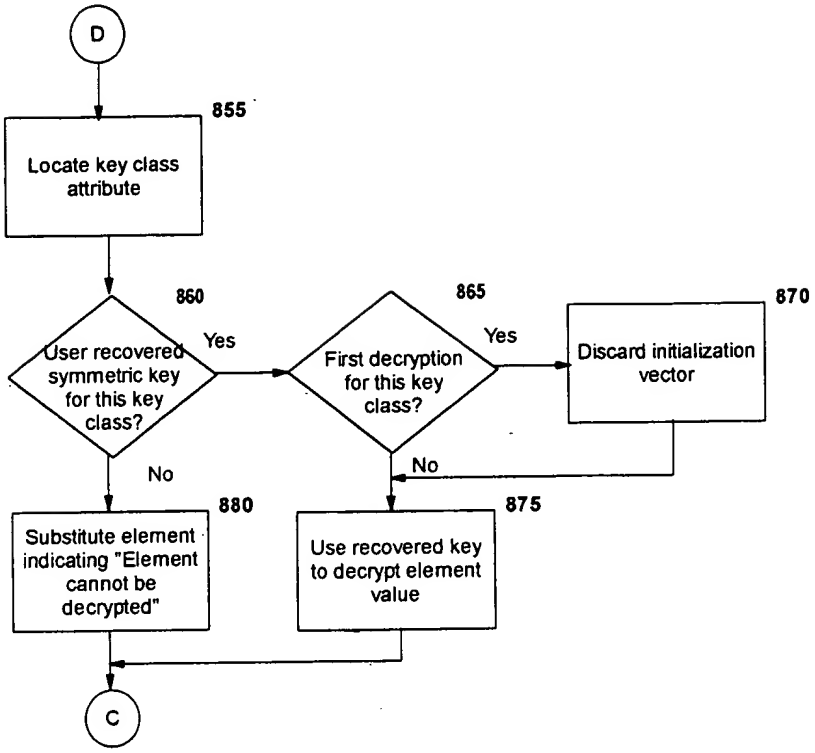

D
855
Locate key class attribute
860
User recovered symmetric key for this key class?
Yes
865
First decryption for this key class?
Yes
870
Discard initialization vector
No
No
880
Substitute element indicating "Element cannot be decrypted"
875
Use recovered key to decrypt element value
C

Fig. 8B

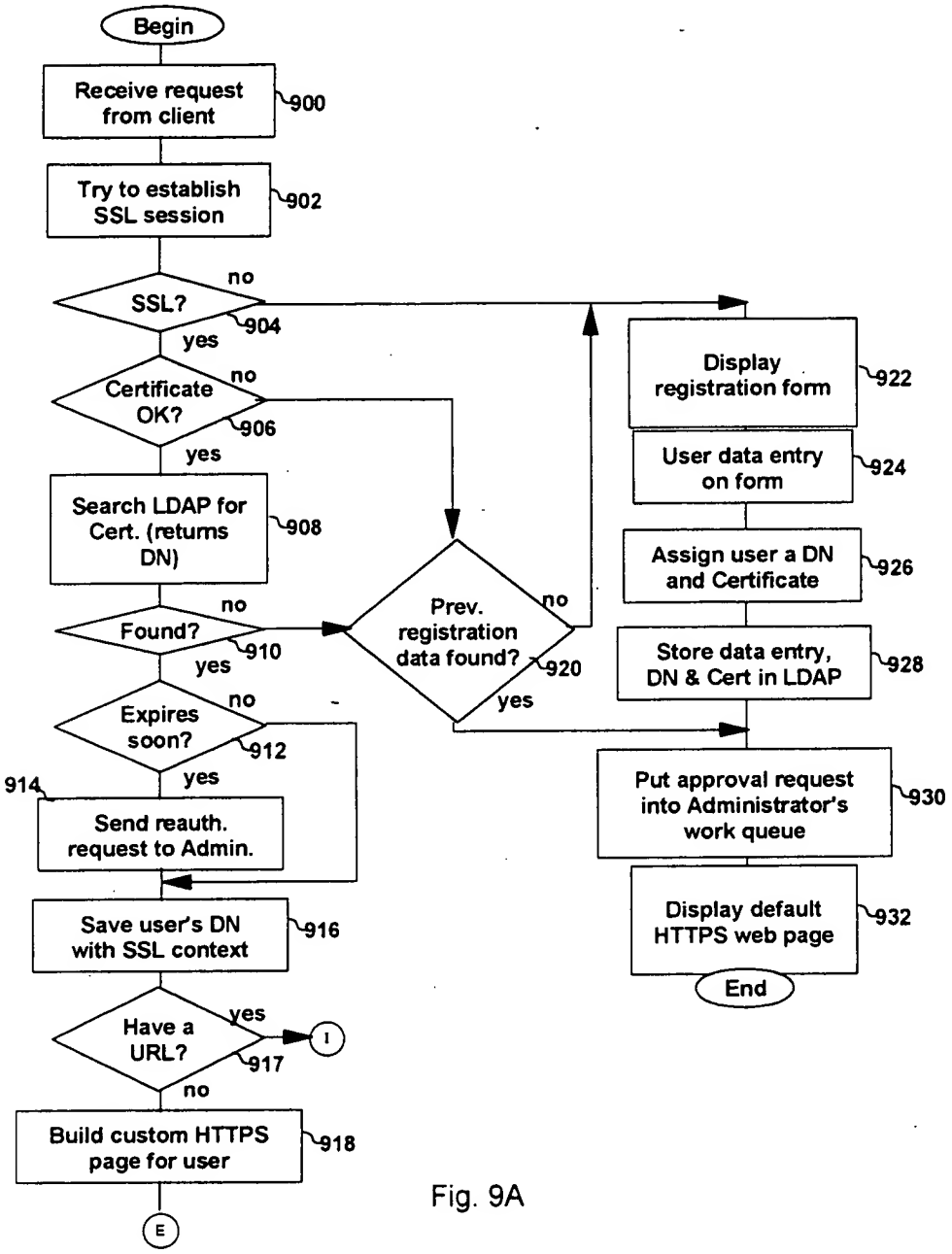


Fig. 9A

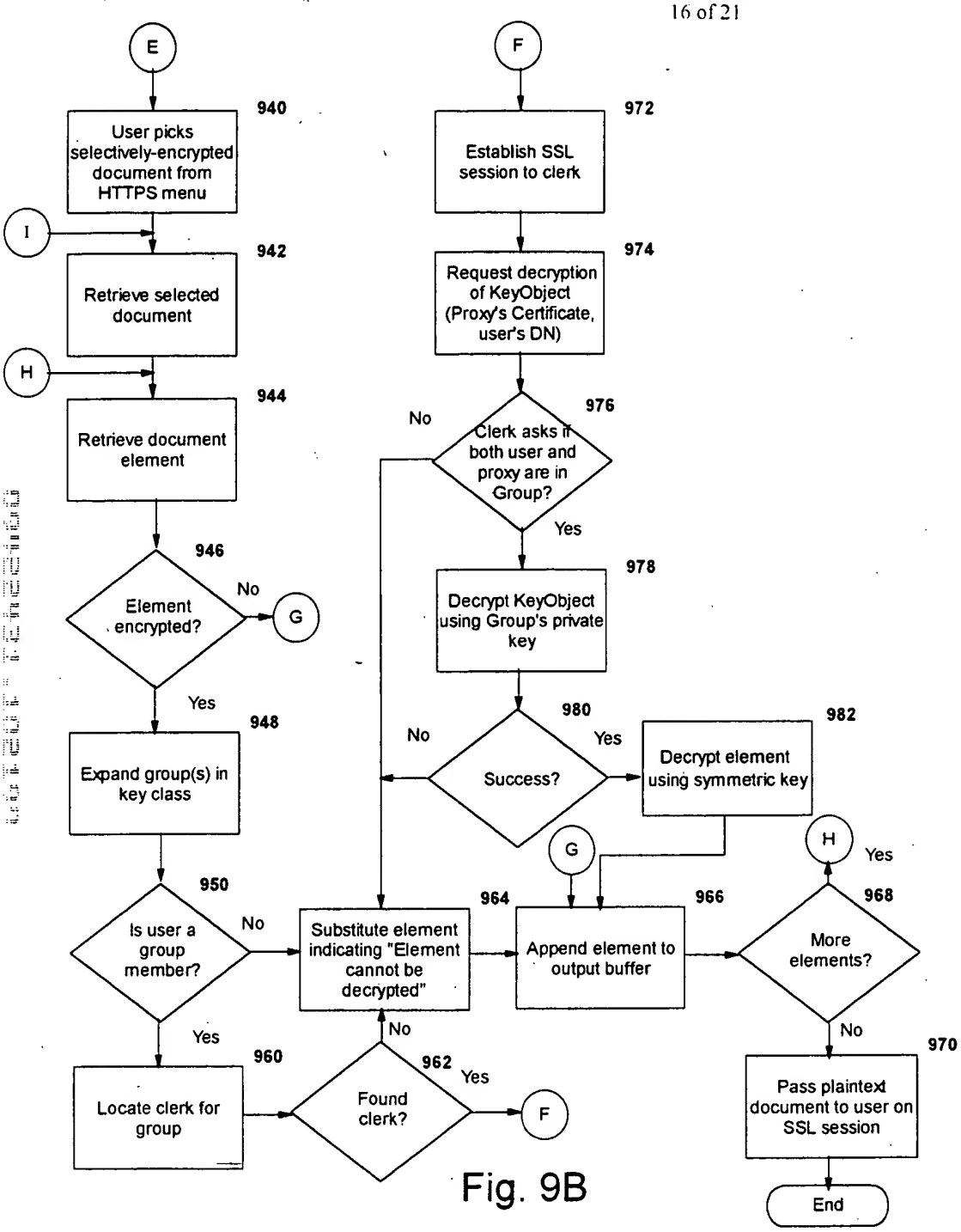

E
User picks selectively-encrypted document from HTTPS menu
940
I
Retrieve selected document
942
H
Retrieve document element
944
Element encrypted?
946
No
G
Yes
Expand group(s) in key class
948
Is user a group member?
950
No
Yes
Locate clerk for group
960
Found clerk?
962
Yes
No
F
Substitute element indicating "Element cannot be decrypted"
964
F
Establish SSL session to clerk
972
Request decryption of KeyObject (Proxy's Certificate, user's DN)
974
Clerk asks if both user and proxy are in Group?
976
No
Yes
Decrypt KeyObject using Group's private key
978
Success?
980
No
Yes
Decrypt element using symmetric key
982
G
Append element to output buffer
966
More elements?
968
H
Yes
No
Pass plaintext document to user on SSL session
970
End

Fig. 9B

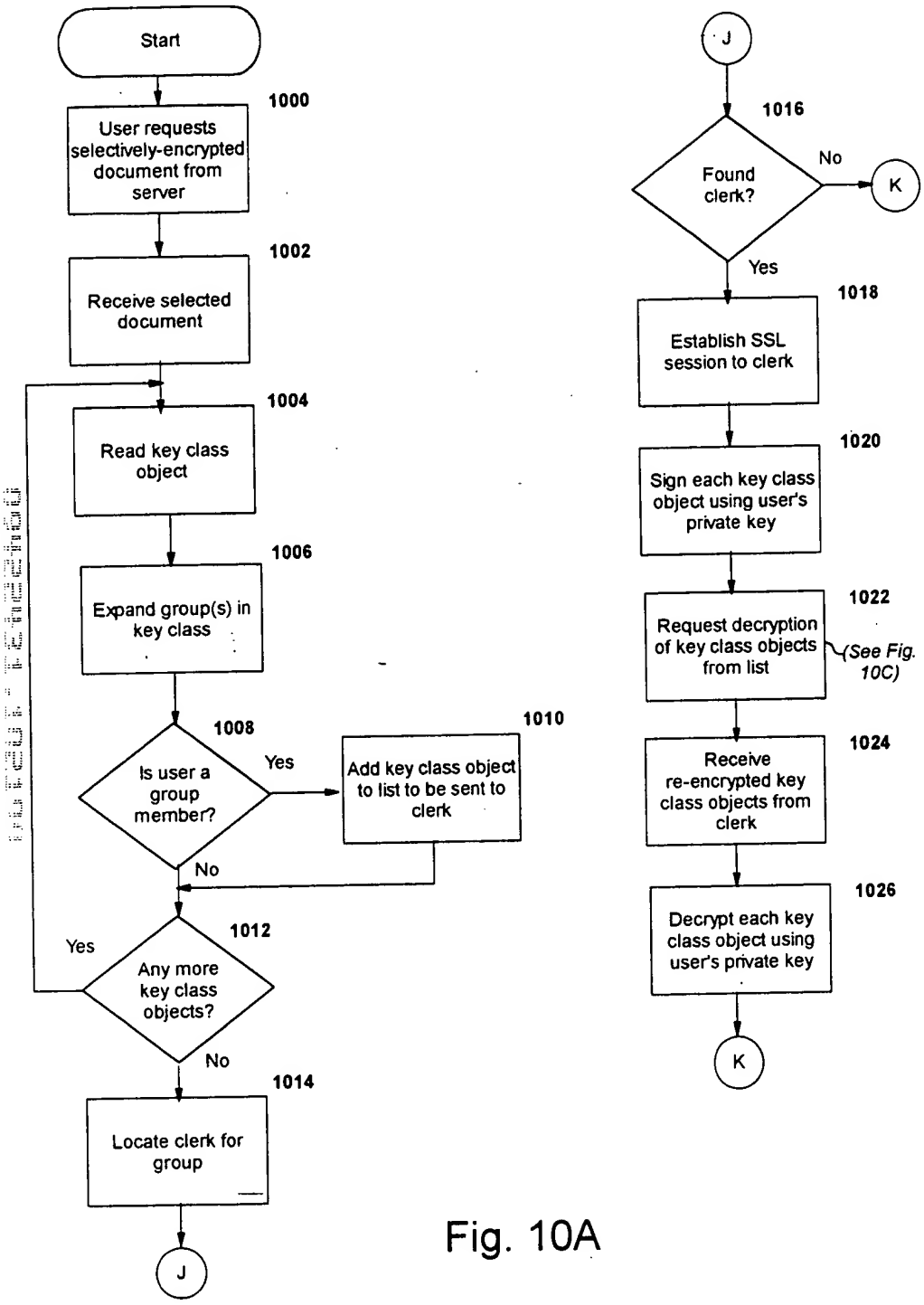

Start
1000
User requests selectively-encrypted document from server
1002
Receive selected document
1004
Read key class object
1006
Expand group(s) in key class
1008
Is user a group member?
Yes
1010
Add key class object to list to be sent to clerk
No
1012
Any more key class objects?
Yes
No
1014
Locate clerk for group
J
J
1016
Found clerk?
No
K
Yes
1018
Establish SSL session to clerk
1020
Sign each key class object using user's private key
1022
Request decryption of key class objects from list
(See Fig. 10C)
1024
Receive re-encrypted key class objects from clerk
1026
Decrypt each key class object using user's private key
K

Fig. 10A

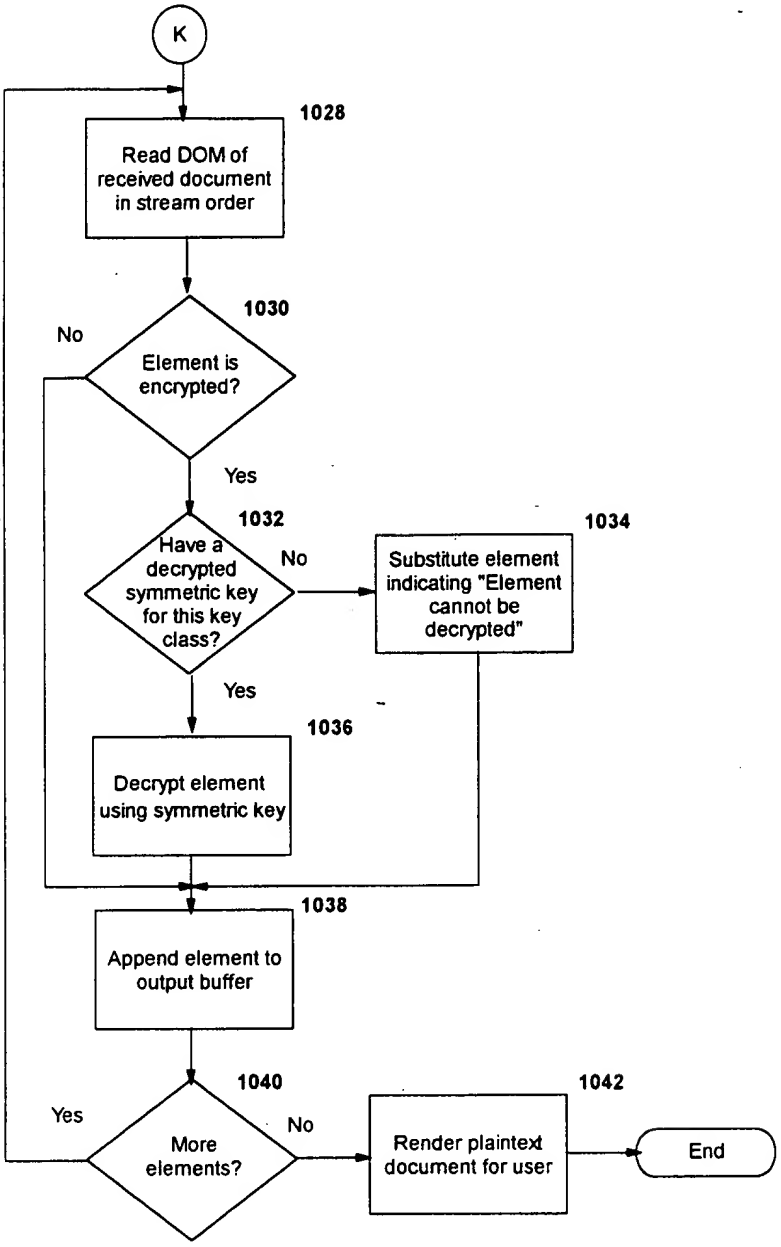

K
1028
Read DOM of received document in stream order
1030
No
Element is encrypted?
Yes
1032
Have a decrypted symmetric key for this key class?
No
1034
Substitute element indicating "Element cannot be decrypted"
Yes
1036
Decrypt element using symmetric key
1038
Append element to output buffer
1040
Yes
More elements?
No
1042
Render plaintext document for user
End

Fig. 10B

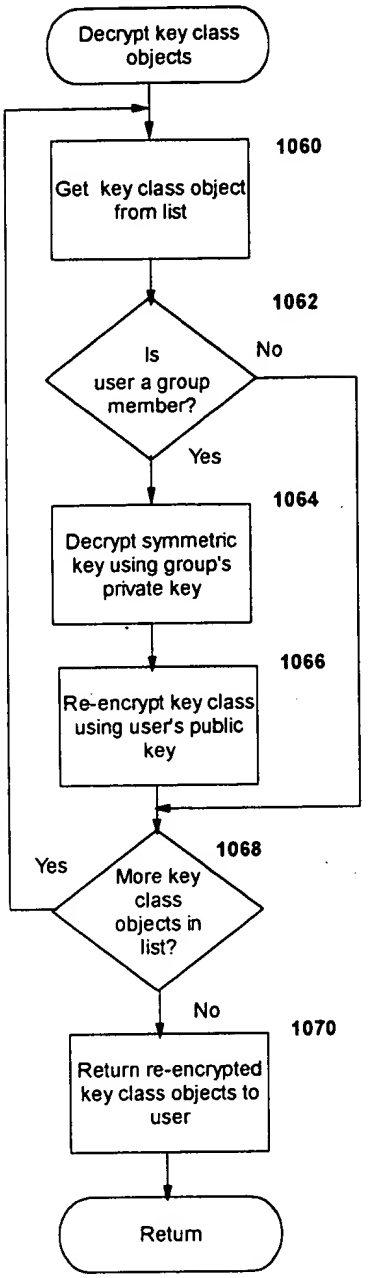


Fig. 10C

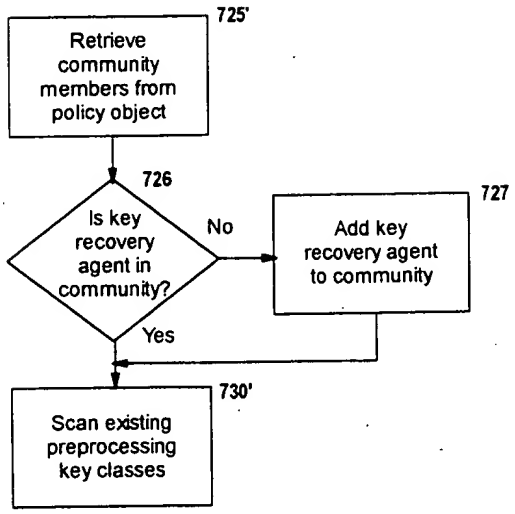


Fig. 11A

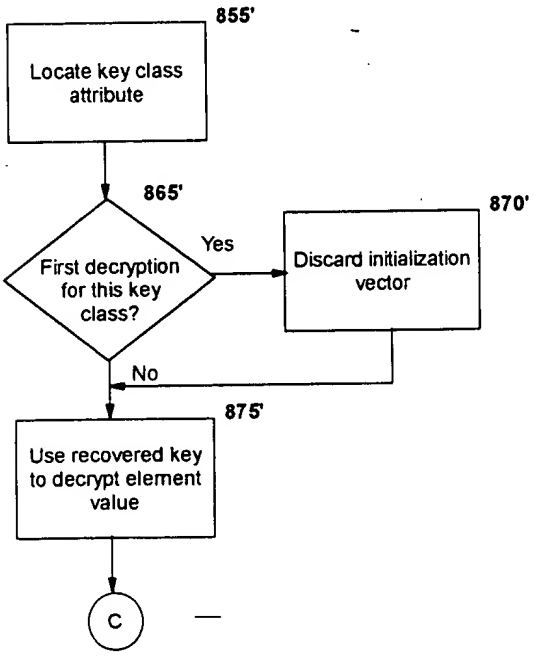


Fig. 11B

Fig. 12